REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-26 are pending in the present application and Claims 1-3, 5, 7, 9, 11, 12, 14-16, 18, 20, 21, 23, 25 and 26 are amended. Support for amendments to Claims 1-3, 5, 7, 9, 11, 12, 14-16, 18, 20, 21, 23, 25 and 26 can be found, for example, in the specification at page 33, lines 5 through 25. Thus, no new matter is added.

In the outstanding Office Action, Claims 1 and 2 are rejected under 35 U.S.C. §103(a) as unpatentable over Lu (U.S. Pat. No. 6,640,108) in view of Saunders (U.S. Pat. Pub. No. 2004/0152446); Claims 3-13, 15-19, and 20-26 are rejected under 35 U.S.C. §102(b) as anticipated by Lauper (U.S. Pat. Pub. No. 2002/0098830); and Claims 14 and 20 are rejected under 35 U.S.C. §103(a) as unpatentable over Lauper in view of Butt (U.S. Pat. No. 6,754,829).

Before turning to the outstanding prior art rejections, it is believed that a brief review of the present invention would be helpful.

In this regard, the present invention describes a wireless communication system which includes a plurality of terminals. In a non-limiting example, shown in Figure 10, the system comprises an ad-hoc network including Terminal A and Terminal B. Terminal A, using the ad-hoc network, sends a beacon signal to Terminal B that includes an identifier, used to identify the type of certificate of privilege, and an operation mode indicator, used to indicate the operation mode of the terminal. Terminal B then responds by requesting authentication using the type of certificate of privilege which matches the identifier and indicates a right concerning the operation mode.

Turning now to the §103(a) rejection in the outstanding Office Action, Applicants respectfully traverse the §103(a) rejection based on Lu and Saunders for the following reasons.

Claim 1 recites, in part,

> an ad-hoc network;
> a first terminal configured to send, using the ad-hoc network, a signal that includes beacon information having an identifier that identifies a type of certificate of privilege; and
> a second terminal configured to send, using the ad-hoc network, an authentication request to the first terminal in response to the signal sent from the first terminal by providing the type of certificate of privilege which matches the identifier.

Claim 2 recites similar features.

Lu describes a private and a public GSM cellular network for cellular communication. Further, Lu describes a switch that monitors calls initiated by a handset and determines if both the initiating handset and the destination handset are within a private network and if so the switch moves the call to the private network saving the usage fees that would be charged for using the public network.[1] However, Lu does not describe an ad-hoc network, nor does Lu describe any terminal configured to send using the ad-hoc network. Further, Lu does not describe a second terminal configured to send an authentication request to the first terminal in response to the signal sent from the first terminal.

The outstanding Office Action relies on Saunders to cure the above noted deficiencies of Lu. Saunders describes a system that allows mobile devices to access an intranet using a wireless application protocol and a unique identifier. However, Saunders does not describe or suggest an ad-hoc network, nor does Saunders describe a first terminal configured to send a signal that includes beacon information having an identifier that identifies the type of certificate of privilege using an ad-hoc network. Further, Saunders does not describe a second terminal configured to send, using the ad-hoc network, an authentication request to the first terminal in response to the signal sent from the first terminal by providing the type of certificate of privilege which matches the identifier.

[1] Lu, Col 14, lines 47-65 and Col. 15, lines 33-56.

In other words, Saunders describes providing secure access from a mobile terminal to an intranet, but Saunders does not describe a first terminal configured to send a beacon to a second terminal using an ad-hoc network, or a second terminal sending an authentication request back to the first terminal in response.

Therefore, it is respectfully submitted that independent Claims 1 and 2 and claims depending therefrom, patentably distinguish over Lu and Saunders.

Regarding the rejection of Claims 3-13, 15-19, and 20-26 under §102(b) as anticipated by Lauper, Applicants respectfully traverse the §102(b) rejection for the following reasons.

Claim 3 recites, in part,

> receiving means for receiving a signal sent from a different terminal including beacon information having an identifier that identifies a type of certificate of privilege from the different terminal; and
>
> authentication request means for sending an authentication request to the different terminal by providing the certificate of privilege stored in the certificate of privilege table that matches the identifier contained in the signal received by the receiving means.

Claims 7, 9, 11, 15, 16, 21, 23, 25 and 26 recite similar features.

Lauper describes a method of storing a certificate of origin, or in other words the public key of a certification authority, in a sim module on a mobile device. Further, Lauper describes verifying the authenticity of the electronic partner certificates (or public keys) issued by a certification authority by using a stored certificate of origin (or a public key of the certification authority) to check the certificates (or keys) sent by the certification authority.[2] However, Lauper does not describe or suggest a mobile terminal that receives a beacon signal sent by another mobile terminal. Further Lauper does not describe sending an authentication request to the different mobile terminal providing a certificate of privilege stored in the certificate of privilege table that matches the identifier contained in the signal received.

[2] Lauper, abstract and Paragraphs 0010-0018.

In other words, Lauper describes receiving partner certificates from a centralized certification authority and checking to see if the certification authority certificate is genuine by comparing the received certificate against a certificate stored on a sim module in the mobile device. In contrast, Claim 3 describes a mobile terminal that sends a beacon signal to another mobile terminal that receives the beacon signal and sends an authentication request to the sending terminal based on the information contained in the beacon signal. Accordingly, Lauper does not describe or suggest the features of Claim 3 described above.

Thus, Applicant respectfully submits that Claim 3 and similarly independent Claims 7, 9, 11, 15, 16, 21, 23, 25 and 26 patentably distinguish over Lauper.

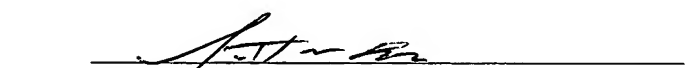
Moreover, with respect to the further dependent Claims 14 and 20, in light of the above discussion, Applicant respectfully submits that those claims also distinguish over the applied art, particularly as none of these further cited teachings to Butt are believed to overcome the above-noted deficiencies of Lauper.

Consequently, in light of the above discussion and in view of the present amendment, the application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Customer Number
22850
Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

I:\ATTY\JL\249225US\249225US_AM.DOC

Scott A. McKeown
Registration No. 42,866